IN THE CLAIMS

Please amend the claims as follows:

1. (Canceled)

2. (Currently Amended) A ~~digital optical~~ storage medium containing ~~compressed digital~~ ~~audiovisual~~ content with protections against unauthorized copying, the storage medium comprising:

~~(a)~~ a digital signature authenticating at least an identifier of ~~said optical~~ the storage medium;

~~(b)~~ a revocations list for identifying at least one ~~other~~ revoked storage medium ~~that is revoked~~;

~~(c)~~ ~~compressed digital audiovisual~~ content that is encrypted by using broadcast encryption, whereby:

~~(i)~~ each of a plurality of authorized playback devices has cryptographic keys sufficient for decrypting ~~said audiovisual~~ the content, and

~~(ii)~~ each of a plurality of revoked playback devices do not have keys sufficient for decrypting ~~said audiovisual~~ the content;

~~(d)~~ program logic for an interpreter of a Turing complete language, the program logic adapted for execution on a playback device in order to play ~~said audiovisual~~ the content,

the program logic ~~installing~~ configured for installation on the playback device; ~~and~~

the program logic further configured for cryptographically authenticating ~~protecting on the playback device~~ the revocations list;

~~(e)~~ a plurality of versions for each of a plurality of portions of ~~said compressed digital audiovisual~~ the content, wherein:

~~(i)~~ said versions for each portion ~~may be~~ are distinguished from each other ~~in pirated recordings of said audiovisual content~~;

~~(ii)~~ said versions are encrypted with different keys, such that each of said authorized playback devices is capable of deciphering at least one, but not all, of said versions for each of said portions; and

~~(iii)~~ the combination of said portions decipherable by a given player ~~may be used~~ usable to identify said player, the program logic being further configured to provide a correct set of decryption keys for decrypting each of said versions; and

~~(f)~~ interface logic defining an interface usable to interact with a user and to control playback of ~~said audiovisual~~ the content.

3. (Currently Amended) The medium of claim 2~~2~~, ~~where~~ wherein:

~~(i)~~ said program logic is configured to perform a plurality of said security checks; and

~~(ii)~~ said program logic is configured to permit playback of ~~said audiovisual~~ the content provided that said plurality of security checks are successful.

4. (Currently Amended) The medium of claim 3 ~~where~~ wherein said program logic is configured to invoke at least one cryptographic operation supported by at least one of said authorized playback devices.

5. (Currently Amended) The medium of claim 3 ~~where~~ wherein said program logic is configured to perform at least one operation necessary for decryption of ~~said audiovisual~~ the content by at least one said authorized playback device.

6. (Currently Amended) The medium of claim 2 wherein a subset of said authorized playback devices encompass a plurality of models, each model having a model-specific vulnerability, and the medium further comprising program logic which, when executed by a device of each said vulnerable model, is configured to:

~~(a)~~ mitigate said vulnerability affecting said vulnerable playback device; and

~~(b)~~ perform at least one operation necessary for said vulnerable playback device to decrypt said audiovisual content.

7. (Currently Amended) The medium of claim 6 ~~where~~ wherein said program logic includes executable code for a Turing-complete virtual machine.

8. (Currently Amended) The medium of claim 6 ~~where~~ wherein said operation necessary to decrypt includes updating a cryptographic key contained in said playback device.

9. (Currently Amended) The medium of claim 6 ~~where~~ wherein said program logic for mitigating includes native executable code configured to detect whether the security of a vulnerable device has been compromised.

10. (Currently Amended) The medium of claim 6 ~~where~~ wherein said program logic for mitigating includes native executable code configured to correct a vulnerability in a vulnerable device.

11. (Currently Amended) The medium of claim 6 ~~where~~ wherein said program logic for mitigating includes a firmware upgrade for correcting at least one vulnerability.

12. (Currently Amended) A device for securely playing ~~digital audiovisual~~ content, ~~said audiovisual~~ the content including a plurality of regions each having multiple versions thereof, the device comprising:

~~(a)~~ a media reader ~~drive including a laser~~ for use in reading data from ~~rotating optical media~~ a storage medium;

~~(b)~~ a nonvolatile memory containing:

~~(i)~~ a set of cryptographic player keys for use with a broadcast encryption system, and

~~(ii)~~ identifiers of revoked media;

~~(c)~~ a bulk decryption module for decrypting encrypted ~~audiovisual~~ content from ~~said media~~ the storage medium;

~~(d)~~ a Turing-complete interpreter for executing program logic, the program logic configured to:

~~(i)~~ install from the media reader; ~~drive and~~

cryptographically authenticate ~~protect in the nonvolatile memory~~ identifiers of revoked media;

~~(ii)~~ verify whether valid digital signatures contained on ~~said media~~ the storage medium authenticate ~~said media~~ the storage medium; and

~~(iii)~~ verify whether ~~said media are~~ the storage medium is identified as revoked in said nonvolatile memory;

~~(iv)~~ select a version of each ~~said~~ of the plurality of regions, thereby generating a set of selected versions;

provide a correct set of decryption keys for decrypting each of said selected versions;

~~(v)~~ decrypt said selected version~~(s)~~, whereby a combination of said versions selected in the course of playing ~~said media~~ content from the storage medium uniquely identifies said device; and

~~(c)~~ at least one codec for ~~decompressing said audiovisual~~ decoding content.

13. (Currently Amended) The device of claim 12 further comprising an interpreter for a Turing-complete language, ~~where~~ wherein said interpreter is configured to obtain said program logic from said drive and execute said program logic.

14. (Currently Amended) The device of claim 12 further comprising means for reducing during a rendering process the output quality of said audiovisual content in dependence upon whether a security requirement specified by ~~said~~ the storage medium for high-quality output is met.

15. (Currently Amended) The device of claim 12 wherein:

~~(a)~~ said combination of versions selected during the course of playback of any one ~~said~~ storage medium does not uniquely identify ~~said playback~~ the device; and

~~(b)~~ said combination of versions selected during the course of playback of a plurality of ~~said~~ storage media does uniquely identify ~~said playback~~ the device.

16. (Currently Amended) A method for playing encrypted ~~digital audiovisual~~ content from a ~~digital~~ storage medium, the method comprising:

~~(a)~~ verifying a digital signature for authenticating said medium;

~~(b)~~ retrieving at least one player key from a nonvolatile memory;

~~(c)~~ using said at least one player key with a broadcast encryption system;

~~(d)~~ using a result of said broadcast encryption system to decrypt at least a portion of ~~said audiovisual~~ the content;

~~(e)~~ reading program logic for a Turing-complete interpreted language from the ~~digital~~ medium;

~~(f)~~ using an interpreter to execute said program logic, wherein said interpreter performs operations specified in said program logic including

~~(i)~~ installing from ~~the~~ a media player device; ~~drive and~~ cryptographically authenticating ~~protecting~~ identifiers of revoked media;

~~(ii)~~ verifying whether valid digital signatures contained on ~~said media~~ the medium authenticate the medium ~~said media~~; and

~~(iii)~~ verifying whether ~~said media are~~ the medium is identified as revoked in said nonvolatile memory;

~~(g)~~ selecting a variant from a plurality of variants for each of a plurality of portions of ~~said audiovisual~~ the content, wherein:

~~(i)~~ said media player device is capable of decrypting said selected variant; and

~~(ii)~~ said media player device lacks at least one cryptographic key required to decrypt at least one non-selected variant for each ~~said~~ portion;

providing a correct set of decryption keys for decrypting each selected variant; and

~~(h)~~ decrypting each ~~said~~ selected variant using the provided correct set of decryption keys.

17. (Currently Amended) The method of claim 16 ~~where~~ wherein said interpreter performs operations specified in said program logic to respond to selections from a user, said user selections include button presses on a remote control.

18. (Currently Amended) The method of claim 16 ~~where~~ wherein said program logic directs said player to perform an AES block cipher operation via said interpreter.

19. (Previously Presented) The method of claim 16 further comprising accessing a media revocations list to determine whether said medium has been revoked.

20. (Currently Amended) The device of claim 12 ~~where~~ wherein:
said set of cryptographic player keys is unique to the player; and
said program logic is configured to select a unique set of versions representing the content using said unique set of cryptographic player keys.

21. (Currently Amended) The medium of claim 3, ~~where~~ wherein the program logic that is configured to perform a plurality of security checks generates a security check result, the security check result for embedding ~~results of the program logic is adapted to embed the results of the at least one security check~~ into ~~audio-visual~~ content rendered by a ~~the~~ playback device on which the security checking is performed.

22. (Currently Amended) The medium of claim 2, ~~where~~ wherein the program logic is adapted to perform at least one security check of a playback device seeking to play ~~said audiovisual~~ the content, the at least one security check adapted to verify at least one of

~~(i)~~ playback device identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or

~~(ii)~~ a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device.

23. (Currently Amended) The device of claim 12, further comprising ~~where the~~ media verification logic ~~further performs~~ configured to perform a security check that interrogates a playback environment to verify at least one of:

~~(i)~~ playback device identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or

~~(ii)~~ a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised playback device.

24. (Currently Amended) The device of claim 12 ~~where~~ wherein the Turing-complete interpreter is adapted to execute program logic that does not decrypt a selected version if the program logic identifies said media as revoked.

25. (Currently Amended) The method of claim 16 ~~where~~ wherein said program logic performs at least one security check of a player device seeking to play said audiovisual content, the at least one security check adapted to verify at least one of:

~~(i)~~ player identity, including at least one of player serial number, specific subscriber information, player model, or player software version, or

~~(ii)~~ a result of cryptographic processing adapted to fail verification operation if executed on at least one of an unauthorized or revoked or compromised player, and to inhibit at least one of full quality playback or playback if at least one security check fails.